CONNECTING THE EDGE:
Mobile Ad-Hoc Networks (MANETs) for Network Centric Warfare

Brent A. Peacock, Major, USAF

April 2007

Blue Horizons Paper
Center for Strategy and Technology
Air War College

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **APR 2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE **Connecting the Edge: Mobile Ad-Hoc Networks (MANETs) for Network Centric Warfare**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,Air War College,Center for Strategy and Technology,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**51**	

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

The principles of Network Centric Warfare (NCW) are at the heart of DoD transformation plans and are the driving concept of several high profile acquisition programs. This paper addresses the question of what communications and networking technology breakthroughs are required to fully realize mobile ad hoc networking (MANET) and deliver on the promises of NCW at the tactical edge of our military forces in the 2025 timeframe. We begin with a review of the background and major principles of NCW to define the key characteristics a NCW enabled force must exhibit. Next, we examine the basic concepts of networks and networking in both the context of network theory and in the specific implementation of fixed wired and wireless computer networks. We then describe the characteristics and challenges of mobile ad-hoc networks in general, and the unique requirements for NCW MANETs specifically. The heart of the paper then examines trends in relevant technologies for MANETs in both the commercial and military spheres, highlighting where the trends converge or diverge. Finally, specific technology investment recommendations are offered to set the stage for the successful development of MANETs to implement the vision of NCW.

Contents

List of Figures

“Now the reason the enlightened prince and the wise general conquer the enemy whenever they move and their achievements surpass those of ordinary men is foreknowledge.”
Sun-Tzu, *The Art of War*

Introduction

Since mid 90s, the Pentagon has centered its transformation efforts on the promises of building lighter, leaner, and more lethal forces using the tenets of Network Centric Warfare (NCW). By using information technology (IT) to connect sensors, shooters, and decision makers together in a common framework, a military force can achieve rapid, concurrent discovery of enemy activities and dispositions. This information superiority underpins the Joint Vision 2010 and 2020 operational concepts of Dominant Maneuver, Precision Engagement, Focused Logistics, and Full Spectrum Protection allowing US Forces to achieve Full Spectrum Dominance over any opposing force.[1] Although the specific IT tools of NCW are new and still emerging, the concept of building and maintaining information superiority is as old as warfare itself. Despite being outnumbered most of the time, the armies of the 13th century Mongols built and ruled the largest continental empire in history through conquest based largely on their “absolute dominance of battlefield information.”[2] Through a deliberate campaign targeting enemy messengers and using their own pony express-like system of arrow riders, the Mongols repeatedly utilized the resultant information superiority to rout their opponents.[3] Today, thanks to the rapid proliferation of IT throughout the military and civilian sectors, information superiority has become even more critical as force sizes decrease and commanders substitute agility for mass as the decisive component of operational and tactical warfare. However, the information superiority that fuels today’s lighter, more lethal military forces is increasingly vulnerable to the innovative use of commercially available IT by network oriented (versus hierarchically structured) adversaries. Modern IT’s ability to deliver substantial, new capabilities to, while also exposing new vulnerabilities in, our military forces, has been central to shaping the discussions of transforming the Department of Defense (DoD) into a NCW enterprise.[4] The NCW movement, which began as little more than thought pieces in military journals and Pentagon white papers in the mid 1990s, has become the central theme in the services transformation campaigns. Evidence of the pervasiveness of this shift can be seen in a quick review of the service budgets. Many ongoing and planned significant defense acquisition programs are based on NCW tenets. The Army's Future Combat Systems is a family of 14 manned and unmanned systems connected by a common network that ties the system of systems together through data, voice, and video communications riding over a common network. The envisioned FCS Brigade Combat Team will utilize "an advanced network architecture that will enable levels of joint connectivity, situational awareness and understanding, and synchronized operations heretofore unachievable."[5] On the Navy ledger, FORCEnet is the command and control operational concept and overriding architectural framework for the Navy's Sea Power 21 initiative. Although not an acquisition program itself, FORCEnet ties together the SEA SHIELD, SEA STRIKE, and SEA BASE concepts by defining the "systems and processes for providing fully networked, naval command and control in 2015-2020."[6] Beyond these service initiatives, the DoD itself is responsible for the largest NCW related project, the core enabling network of networks itself, the Global Information Grid (GIG). The GIG is designed to provide the so called "entry fee" for NCW, the densely interconnected, ultra-high bandwidth, highly reliable information infrastructure, or "infostructure" into which the FCS, FORCEnet, and other NCW systems will tie.[7] However, the GIG acquisition is primarily focused on providing a long haul, fixed, high bandwidth, secure backbone for military networking and communications. In order to truly achieve the goals of NCW, all the individual, generally mobile, warfighting entities

– tanks, aircraft, UAVs, soldiers, unattended sensors, indirect fires systems, and C2 assets – must be integrated into the grid. This is not a superficial integration that aims to merely pass simple voice communications and a smattering of digital data. Truly NCW-compliant integration will feature a densely linked network of networks with high bandwidth and sufficient quality of service (QoS) to provide a common view of the battlespace to all network nodes, especially the tactical edge nodes. Interconnecting these edge nodes will rely upon mobile ad-hoc networking (MANET) technologies. It is necessary to understand the capabilities required to develop and field NCW enabled forces in order to determine the specific technological requirements for developing the MANETs that will connect the tactical edge of the military enterprise: the sensors, enablers, and shooters that will perform the military mission.

The first section of this paper will briefly discuss the background of NCW and the desired characteristics of a NCW enabled force. Next, the basic concepts of networks and networking will be examined in both the context of network theory and in the specific implementation of fixed wired and wireless computer networks. It will then describe the characteristics and challenges of mobile ad-hoc networks in general, and the unique requirements for NCW MANETs specifically. The heart of the paper then examines trends in relevant technologies for MANETs in both the commercial and military spheres, highlighting where the trends converge or diverge. Finally, specific technology investment recommendations are offered to set the stage for the successful development of MANETs to implement the vision of NCW.

Network Centric Warfare Background and Characteristics

The concept of Network Centric Warfare has been known by many different names – cyber war, command and control (C2) warfare, cognitive dominance, distributed network operations, etc. – each with slightly different, but highly overlapping definitions. The many names reflect the struggle of military and strategic thinkers to fully describe the significance of the phase shift in warfighting doctrine that this philosophy represents. The late Vice Admiral Arthur Cebrowski and Mr. John Garstka are generally credited with introducing the concept and origins of NCW.[8] They described the military's evolution from platform-centric to network-centric forces as an inevitable outgrowth of the United States' economic and societal evolution driven by the shift from industrial age to information age philosophies, processes, and tools. Information technology has altered the business and economic environment by providing ubiquitous communications, low-cost, high-power computer processing, cheap, high-volume data storage, a proliferation of sensors, and advanced software capabilities that collectively provide precise, readily available information on the operating environment. Of course, just having IT tools is not enough. To fully utilize the advantages that IT can provide, a business must also possess the appropriate culture, organizational structure, and set of processes to effectively wield these tools to obtain a competitive advantage. With precise information on market demand, inventory levels, commodity prices and availability, and enterprise, if not world-wide, visibility of manufacturing capacity, businesses are now utilizing IT to rapidly adapt to changes in their environment, or eco-systems in the vernacular of Cebrowski and Garstka, in order to obtain an advantage in their markets.[9] In a word, a business with the right organization, processes, and IT fueled tools can achieve the ultimate competitive advantage: agility.

Agility can be defined as the ability to move quickly, but in a sure-footed manner.[10] Agility of forces, organization, resources, and command and control are the fundamental attributes that information age forces must strive to achieve. The advocates of NCW propose that the most effective and efficient means to enable agility is the establishment of shared awareness and full collaboration amongst all the entities in an organization.[11] Shared awareness and collaboration require robust communications and rapid exchange of data via one or more networks. The complete networking of battlespace entities is the key enabler to achieving these effects and is the cornerstone of NCW. As the Assistant Secretary of Defense for C3I's Command and Control Research Program asserts, "NCW focuses on the combat power that can be generated from the effective linking or networking of the combat enterprise."[12] These agile, richly connected enterprises will exhibit the NCW characteristics of speed of command, massing of effects, cooperative engagement, high tempo and responsiveness, and self-synchronization to a degree that cannot be matched by any non-NCW capable opponent.[13] Although effectively implementing IT is a central tenet of NCW, it is important to remember that NCW is not solely a technologically driven phenomenon. The processes (doctrine), organizational structure, and culture of an organization are critical enablers to the proper utilization of the tremendous tools presented by the on-going trends in IT of increased processing power, smaller form factors, and lower costs. To proceed with the implementation of NCW by simply pursuing the technology pieces alone would ultimately fail. However, in the end it is the network that defines NCW, and therefore understanding how to best design, implement, and protect these networks is the critical materiel piece of the NCW transformation. Put more directly by one leading DARPA program manager, "the network is the most important weapons platform for the military of the future."[14]

Networks: Background and Definitions

In some circles, the *network* in Network Centric Warfare is associated solely with computer or communications networks. Unfortunately, this emphasizes the technological aspect of NCW at the expense of the more profound implications of network organization, theory, and behavior for military utility. In this section, we will examine some basic principles of network theory and discuss why they are important to NCW, define wired and wireless computer networks in general, and then define Mobile Ad-Hoc Networks and describe their specific components and functions.

Networks and Network Theory

The study of networks, or network theory, is an outgrowth of the mathematical study of graph theory and is “a fundamental pillar of discrete mathematics.”[15] In mathematics, a graph is a collection of vertices (or nodes) connected by edges (or links). Where a graph, or simple network, may reflect basic connectivity among a trivial number of nodes, more complex networks can be used to use relationships, or exchanges of information among many hundreds to many millions of nodes. Interconnectivity models consisting of complex networks are used throughout the physical, social, and computer sciences as tools for representing relationships and data flows.[16] A network’s topology, one of a network’s fundamental defining properties, defines these relationships or data flows. A topology is the architecture of the connectivity of a network’s nodes. There are many different types of possible topologies, but this paper will focus on three of the most basic: star, full mesh, and partial mesh. Star topologies have a single central node that connects to every other node in the network. In full mesh topologies, every node directly connects to every other node in the network. A partial mesh is a network with some nodes connecting to multiple nodes.

Beyond these basic topological forms, complex networks can also be described in terms of their performance by using five characteristics: characteristic path length (CPL), link/node ratio, clustering, scale, and diffusion rate.[17] These characteristics are fully defined in Appendix A. From a NCW viewpoint, network theory provides the methodology to define desirable attributes for network performance using the first four of these characteristics. The fifth characteristic, diffusion rate, is derived from the first four characteristics and is therefore not considered as an independent design point. In order to reduce latency in a network, communications should use the shortest possible routes between sending and receiving nodes. Assuming comparable transmission costs for all links in a network, it follows that networks with low CPLs will have lower latency than high CPL networks. Given that, it would seem a high link/node ratio would be desirable in order to achieve a low CPL, as more links would generally equate to shorter lengths from one node to another. However, it has been shown that networks with a link/node ratio of about 2 are able to perform similarly to networks with much higher link/node ratios but require less overhead for link maintenance and protection.[18] Networks with high clustering coefficients usually have localized regions of dense connectivity that contribute to the overall robustness of the network. A clustering coefficient of 0.25 or greater (1 is the maximum) is desirable for reliability purposes[19]. Networks exhibiting scale, or an even distribution of links among nodes, are more susceptible to disruption from the loss of several nodes than scale free or skew degree distribution networks. A network with skew degree distribution will have a very small number of nodes with a very large number of links, a moderate number of nodes with moderate number of links, and a very large number of nodes with very few links.[20] Networks with skew degree distribution tend to have high clustering coefficients. The combination of these characteristics yields robust, readily re-configurable networks.[21] We will re-visit these performance characteristics when we address the trends and challenges in the networking technology later in this paper.

Computer Networks

In its most basic form, a computer network is three or more computers connected via a communications system for the purpose of sharing data and/or resources, such as a printer. Although the communications systems used to build a computer network can vary, by far the most common types are based on the Open Systems Interconnection Basic Reference Model or OSI Model for short. The OSI Model was developed by the International Standards Organization beginning in 1977 and is characterized by the seven-layer network abstract model as shown in figure 1.[22]

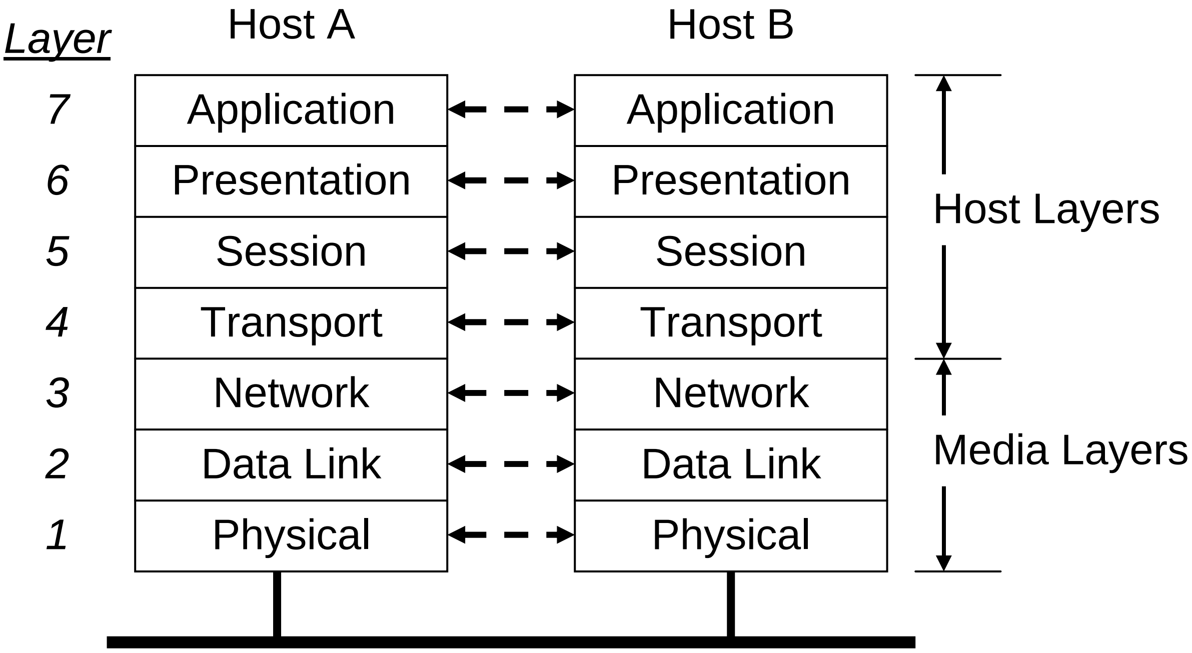

Figure 1: The Seven-Layer OSI Model

Each layer provides specific functionality for the overall networking protocol. A given layer's functionality is implemented by one or more entities (either software, hardware, or both, dependent upon the specific layer) which provide services to the neighboring higher layer and communicate directly only with entities in the next lower level. The entities in each layer in the model may only communicate with the layer immediately above or immediately below inside the same host (computer or node) or with the same layer of a different host (e.g. the network layer in host A in figure 1 may communicate only with the transport layer or data link layer in host A or the network layer in host B). The OSI seven-layer model underlies every popular networking protocol. The OSI model was developed as an extension of the original five layer Transmission Control Protocol and Internet Protocol (TCP/IP) protocol suite that served as the heart of the ARPANET, the first large-scale, long distance computer network developed by DARPA that eventually morphed into today's Internet. The Application, Presentation, and Session layers of the OSI Model are encapsulated in the Application layer of the TCP/IP protocol. The remaining layers are consistent between the OSI Model and TCP/IP.

The bottom layer, or layer 1, of both the OSI Model and the TCP/IP protocol is the physical layer. The physical layer defines all the electrical and physical specifications for connectivity in a network.[23] One of the primary functions this layer provides is the conversion of digital data into the appropriate electrical signal for transmission over a communications channel. This signal may be particular voltage on a wired copper cable, a certain wavelength of light for a fiber optic cable or open-air laser, or a specific analog signal for a radio link. The key is that from an overall network perspective, the actual physical connection from one host to another is immaterial and, ideally, invisible to the network as a whole.

Wired Computer Networks: Advantages and Disadvantages

Computer networks consisting of wired layer 1 connectivity are by far the most prevalent. The core of both the Internet and the DoD's GIG consist of high capacity, high bandwidth fiber optic based cabled networks. Advantages of wired networks include: 1) general immunity to interference from other signal sources, 2) enhanced physical security of the network (i.e. you have to be physically connected to a network device by a cable in order to access it), 3) generally linear scalability, 4) high speed (low latency) and 5) high bandwidth. The disadvantages of wired networks are: 1) physical space required for cabling, 2) inflexibility in redeploying existing nodes, 3) initial acquisition and maintenance costs of cabling, and 4) "tether" factor of being tied to a cable.

Wireless Computer Networks: Advantages and Disadvantages

Primarily due to the disadvantages listed above, wireless RF based line of sight (LOS) networks are increasingly utilized at the edge of the Internet and in localized LANs in place of wired connectivity. These wireless nets, normally built with commercially available wireless routers and network cards based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 series of standards collectively known as Wi-Fi (wireless fidelity), allow greater flexibility in deploying new nodes or redeploying existing ones without having to acquire or adjust a large wired infrastructure. However, the cost benefits and ease of use associated with wireless networks come at the price of limited bandwidth, limited range and connectivity difficulties due to environmental factors, and security concerns.

The physical layer media utilized by wireless networks, the RF spectrum, imposes significant limitations on available bandwidth. Wired internet technology is based on scalable media (i.e. hubs and routers connected primarily by fiber optic cables) while wireless nets must contend in the increasingly crowded RF spectrum.[24] Consider that a single typical fiber optic bundle, utilizing multiplexing, can carry approximately 200,000 GHz of analog bandwidth, while wireless devices can generally use less than three GHz of RF spectrum, and the DoD is restricted to just a few hundred MHz total![25] When the wired internet requires more bandwidth, it is a relatively simple matter to add more fiber and hubs. Wireless networks, however, are constrained by a zero-sum RF spectrum.[26] Along with limited bandwidth, wireless networks also suffer from limited point-to-point communications range due to atmospheric absorption and attenuation of RF signals.

In a typical commercial wireless network, the effective distance between the network nodes is a few hundred feet at best. Current wireless networks are predominantly of the star or mesh topologies that were discussed previously. A basic commercial wireless LAN utilizes a star topology with a central node known as a router or hub. This topology minimizes the communication overhead for the non-router nodes, as they need only directly interface with the router. The simplicity of this topology is offset by the limitation that each individual node must be able to communicate with the router, thus limiting the overall coverage area of a given network. To overcome this limitation in a star topology, wireless repeaters can be used to extend the router's effective range. An alternative approach is to use a partial or full mesh topology. In these configurations, some nodes, in a partial mesh, or all nodes, in a full mesh, act as routers for their neighboring nodes. As long as a given node, *n*, can reach another node, *p*, that is acting as a router in the mesh, then node *n* remains in the network. Although mesh topologies can significantly increase the effective range of a wireless network, they also impose bandwidth impacts and scalability limits on the network due to the additional workload associated with the routing nodes. Regardless of topology, wireless networks, like all RF applications, are naturally impacted by environmental factors – man-made or natural terrain features, other RF devices competing for the same or nearby frequencies, and broadband interference sources such as microwaves – that can impact network connectivity.

Security is also a significant concern for wireless networks since they possess no inherent physical security measures. With the right equipment, anyone can access the RF signals and potentially obtain entry into the network. Most of the open commercial wireless standards have some level of security incorporated into them by means of encryption. The widely used 802.11 series standards include Wired Equivalence Protection (WEP), a lightweight encryption method that utilizes a simple stream cipher, called RC4, with either a 64 or 128-bit encryption key. However, WEP and its follow on, Wi-Fi Protected Access (WPA), provide minimal protection from a military security standpoint.[27] Recognizing the need for stronger encryption, the 802.11 standards committee responded by developing 802.11i (known as WPA2) which replaced the RC4 encryption core used in WEP and WPA with the Advanced Encryption Standard (AES). Although WPA2 is a significant improvement in security, it comes with the cost of increased administrative burden for a network. WPA2 enabled networks require every user to be given a passphrase. While this is manageable for fixed, closed systems, it becomes a significant headache for enterprise level networks with transient (e.g. internet cafes, libraries, airports, etc.) or dispersed users. In addition to any security measures inherently provided by the network, the nodes themselves can additionally encrypt the data stream being passed through the network. By utilizing a technique known as tunneling, which encrypts the data at the source using a method that is known to the intended recipient, network nodes can establish a virtual private network (VPN). VPNs can effectively enhance network security, but once again, at the cost of total network performance, as the overhead associated with VPNs increases the amount of data that must be transmitted. Collectively these bandwidth, range, access, and security limitations are significant wireless network constraints and are the key drivers of current and future network technology and design research.

Mobile Ad-Hoc Networks

Mobile Ad-hoc Networks, simply stated, are unplanned, self-organizing networks composed of mobile nodes that utilize mesh networking principles for interconnectivity. In this section, we will examine the advantages and disadvantages of MANETs, and then decompose a MANET into its major functional components as a lead in to the MANET technology trends and challenges discussion that follows later in this paper.

MANETs offer several significant advantages to a military force. A MANET's ability to self-form and self-manage eliminates the need for intensive central management of network links, thus reducing support personnel and equipment requirements in forward located areas. By their very nature, MANET technologies allow a force of mobile nodes to more easily share data and attain greater situational awareness than a non-networked force. This increased situational awareness is the cornerstone enabling capability for the NCW tenets of cooperative engagement and self-synchronization discussed earlier. These benefits, however, do not come without some disadvantages.

MANETs suffer from the same limitations as fixed wireless mesh networks, but also are vulnerable to additional challenges resulting from their inherent mobility. As discussed previously, one of the strengths of traditional wireless networks is the ease of user node mobility. The critical distinction between a typical wireless network and a MANET is the wireless network's primary routing infrastructure tends to be static around a fixed entry point into the Internet. In a MANET, the entire network infrastructure is moving along with the user nodes. As the nodes move, point-to-point links may be dropped due to terrain interference or simply because they move beyond range of other nodes. Network stability is continually stressed as nodes drop in and out of the mesh. MANETs may also have limited access to fixed GIG entry points, which ultimately diminishes, but does not eliminate, the overall capability of a MANET while “disconnected” from the broader GIG.

In order to evaluate the specific technologies that enable MANETs, it is useful to functionally decompose a MANET into the first four layers of the OSI model – specifically, the hardware and software that implement the physical layer (layer 1) and the hardware and software of that implement the data link (layer 2), network (layer 3), and transport (layer 4) layers. Referring back to our OSI Model discussion, the physical layer is the actual physical manifestation of the communications bit stream. For MANETs, the bit stream can consist of RF signals or photons. In order to simplify the discussion, we will collectively refer to the physical layer implementations as radios, and the data link, network, and transport layers implementations as the network. Prior to delving into the relevant trends in the technologies related to these components, the next section will help us establish the MANET capabilities that are required to achieve the promises of NCW.

Desired MANET Characteristics for Objective NCW Enabled Forces

In order to operate effectively in the wide range of potential combat environments, future military forces will depend on MANET technologies to achieve the promises of NCW. To deliver the capabilities that NCW enabled forces require at the tactical edge, an objective MANET must possess four general characteristics: strong connectivity, very high bandwidth, effective security, and survivability.

As described in the above section on computer networks, connectivity is at the heart of networking. Our objective NCW MANET will be capable of utilizing multiple physical layer links for both LOS and NLOS connectivity. These links may be simple RF analog links, similar to today's 802.11 standards or JTRS waveforms, or they may be free-space laser links, or a combination of the two. To compensate for terrain or weather effects that might prevent direct point-to-point connectivity between nodes, the objective MANET will utilize airborne nodes (manned or unmanned) and satellite links for NLOS connectivity, and be capable of switching rapidly between these LOS and NLOS links as the MANET nodes move in relation to one another. The objective MANET must be resistant to broadband and spot jamming in order to maintain network coherence. Although the objective MANET strives to reduce latency as much as possible, it must also be tolerant to intermittent high latency and even multiple node disconnects and re-entries to the network. Finally, our objective MANET's connectivity must be highly scalable, encompassing thousands of nodes, or more, in order to reach NCW's goal of a fully networked battlespace.

Connectivity alone is, of course, not sufficient. Our fully connected combat force must also have large amounts of bandwidth at its disposal to effectively achieve shared situational awareness. Today's combat networks are already experiencing huge spikes in demand for bandwidth as data, voice communications, and video converge. Making matters worse, some of the emergent key NCW enabling technologies, like UAVs, are among the most bandwidth intensive applications we have. Not only do UAVs produce huge amounts of high-resolution imagery and full-motion video, which consume bandwidth for transmittal back to their ground stations, but they also demand a large swath of "relatively clear" bandwidth for command and control.[28] This demand will grow non-linearly as the number of network nodes continues to increase per the NCW vision. This expectation has been borne out by the bandwidth demand growth witnessed between DESERT STORM and Operation IRAQI FREEDOM (OIF). During DESERT STORM in 1991, the total bandwidth put into the theater was about 100 Mbps, which served a force of approximately 540,000 personnel.[29] Just twelve years later, the 350,000 troops in theater for OIF were provided 4.2 Gbps (over 40 times more) and it was considered barely sufficient.[30] In order to meet this voracious bandwidth appetite, our objective MANET requires: 1) access to more bandwidth through new link technologies, 2) the ability to dynamically allocate bandwidth between nodes, and 3) the capacity to locally trade connectivity for throughput as the situation, and the specific applications that the MANET is executing, demand. However, even a perfectly connected, unlimited bandwidth MANET is virtually worthless if it is unsecured against intrusion.

The notion of operational security dates back to the earliest days of warfare. In *The Art of War*, Sun-Tzu makes frequent mention of the importance of withholding knowledge of intent or disposition of friendly forces to the enemy. Likewise, protecting the integrity and security of one's command and control (C2) capability is a preeminent concern of most organizations, private or public. The exposed nature of MANETs' connective links makes security of prime importance. An objective MANET requires protection from eavesdropping and malignant code (viruses and worms) to maintain secrecy and integrity. Robust encryption is typically the first line of defense for any communications network, and has been a strength of US Government research and development for many years. On the other hand, as a result of the openness of the Internet, the private sector generally has been in the lead in the battle to detect and counter new computing viruses and worms. In the cases of both encryption and anti-virus/anti-worm techniques and technologies, these protections come at the cost of network performance and must be balanced against the relative threat level and the operational need for low latency and high bandwidth.

Closely related to security is our final characteristic of survivability. Typically, security is an enterprise wide concern aimed at the network as an entity, while survivability is more concerned with protecting individual network nodes. In the MANET context, survivability is directly linked to observability. In order to participate in a MANET, a node must communicate, which means it must radiate a signal of some type. Since radiating in the electromagnetic spectrum in unfriendly territory is an excellent way to become a target, our objective MANET must be capable of staying connected using signals with a low probability of detection (LPD) and a low probability of interception (LPI). The most common LPD/LPI methodology utilizes frequency hopping and spread spectrum techniques. Frequency hopping spread spectrum (FHSS) techniques are widely used in both commercial and military communications. FHSS works by splitting a source signal into multiple lower strength signals that are spread along a band of frequencies that are quickly switching in a pseudorandom manner that is known by both the transmitter and the receiver. The combination of low power and rapid hopping among different frequencies makes these signals difficult for a third party to pull out from background noise. Since these techniques allow multiple devices to utilize the same frequency band with minimal interference, FHSS is at the heart of the Wi-Fi and Bluetooth networking standards and is used in virtually every cordless telephone.[31, 32] On the military side, in addition to LPD/LPI and multi-user properties, FHSS also provides communications that are highly resistant to jamming. Aside from signal processing techniques such as FHSS, another very effective method of achieving LPD/LPI profiles for electronic emissions is to control the direction and shape of the emitted energy. RF antennas can be designed to produce small side lobes and project most of their energy in an intended direction. This technique, known as beam forming, not only reduces the observable emission pattern of an antenna, it can also be used to extend the transmitting and/or receiving range of the system. Open-air laser links are even more effective than RF beam forming in providing stealthy communications. By their very nature, lasers have excellent LPD/LPI characteristics as they consist of very narrow beams that do not produce side lobes. In both instances, the MANET application is hindered by the need for each node to know the relative location of itself to the other nodes, which levies additional processing and communications overhead on the networked force. By defining an objective MANET using these four axes – connectivity, bandwidth, security, and survivability – we can now examine specific trends and research goals in the technologies that potentially provide these characteristics.

Challenges and Trends in MANET Research

Our examination of MANET technology trends encompasses both the commercial and defense sectors as they relate to the two major functional components we introduced in the MANET background section. The first are the physical layer implementations, which we will refer to as radios. The second are the data link, network, and transport layer implementations, which we will collectively refer to as the networks. The utility of the technologies under review will be evaluated using the four required characteristics of the objective MANET as detailed in the preceding section: connectivity, bandwidth, security, and survivability. We now begin our study of MANET specific challenges and the current and projected commercial and military research efforts to overcome them in the field of radios.

Radio related challenges and research efforts

On the radio side of the MANET ledger, the commercial and defense markets have enjoyed a synergistic relationship, with specific requirements from one market providing new capabilities to the other. The proliferation of wireless voice and data communication devices and the scarcity of available RF spectrum drive commercial vendors to seek out many of the same innovations as military researchers. Turning to our required MANET characteristics, the commercial market shares the DoD's strong interest in two of the four: connectivity and bandwidth. Privacy concerns drive a fairly strong commercial interest in improving wireless security, but not to the extent of meeting military security requirements. The final characteristic, survivability, does not have a direct commercial market (excluding criminal organizations) but many of the techniques and technologies that exhibit LPI/LPD properties also have desirable spectrum sharing capabilities (e.g. FHSS) and therefore are also addressed to some degree by commercial research. To further facilitate our examination of radio technologies, radios can be decomposed into receiver/transmitters (R/Ts), digital basebands (signal processing cores), and network/processor interfaces. Though there are many radio technologies that lend themselves to MANET implementation, the core radio research thrust for both the commercial and defense markets is in the field of software defined radios.

The Software Defined Radio (SDR) initiative is an outgrowth of the DoD's Joint Tactical Radio System (JTRS) Program. Begun in the late 1990s, the original JTRS program intent was to replace the multitude of service-specific legacy radios with a single system that would allow full interoperability between the services.[33] However, because of the momentum of NCW driven transformation efforts, the JTRS program scope began to rapidly expand, including, among other things, the inclusion of MANET requirements. Over time, the JTRS program plan has evolved into an incremental delivery of the full requirement set, with full concurrence among the services of initial MANET capability being the highest requirement for Increment 1.[34] The key technology for meeting the JTRS program requirements is SDR. SDRs are an effort to separate a radio's waveform – the functions that occur from user input to radio frequency output, and vice versa[35] – from the radio's physical hardware. The SDR Forum, an industry association dedicated to the development of global standards for SDR development and deployment, defines an SDR device as one that can be dynamically programmed in software to reconfigure the characteristics of hardware to perform different functions at different times.[36] The goal is a core set of radio hardware with a well-defined collection of application programming interfaces (APIs) that provide a stable interface for specific software defined functionality, i.e. specific RF waveforms. So as a new generation of any given communication protocol is developed, a communications enterprise can simply upgrade the software on their existing hardware infrastructure, saving huge amounts of money and time. Beyond the DoD's needs, the tremendous costs associated with upgrading network infrastructure from one generation of cellular service to the next (about $1 billion to transition from 2G to 3G networks[37]) has provided a huge commercial incentive for SDR technology as well. Although simple in concept, the actual development of waveform apathetic hardware is difficult in execution. Designers need to minimize the R/T section in terms of complexity and number of analog components to yield an SDR that "performs carrier-speed data conversion and operates on signals exclusively in the digital domain."[38] To meet these design goals in RF R/Ts, significant advances are required in high-speed analog-to-digital (ADC) and digital-to-analog converters (DAC), digital upconversion and downconversion techniques and speeds, and tunable antennas. Development is already underway for very high-speed ADC chips using microelectromechanical system (MEMS) circuits that will be capable of processing hundreds of megahertz of RF spectrum simultaneously.[39] As MEMS shrink into the nano scale, NEMS based arrays of digital signal processors (DSPs) will offer even more bandwidth. Once the signal is downconverted into the digital realm, field programmable gate arrays (FPGAs) and arrays of DSPs on single ICs can readily perform the necessary processing based on projected improvements of IC densities and operating speeds.[40] On the software side, the JTRS program has mandated vendor compliance with the Software Communications Architecture (SCA) to ease interoperability and encourage co-development inside industry and is strongly pushing for widespread commercial adaptation of SCA.[41] Aside from the DoD, SDR also has a significant government advocate in the FCC, which put processes into place in September 2001 for the review and approval of SDR based products. [42] The commercial market has responded, as the first FCC approved SDR base station was released in 2004 and SDR based cell phones are expected to appear by 2010.[43] Just as today's newest laptops are universally equipped with Wi-Fi and/or Bluetooth networking hardware, it seems self-evident that the maturation of R/T front end technologies and SDR software architectures will provide SDR capabilities to essentially any device with sufficient processing power by 2025. Based on current computing and micro/nanoelectronics trends, SDR technologies will likely be widely available in mobile devices and in fixed communications infrastructure before 2025. While SDR is a crucial technology for eliminating many of the issues associated with legacy hardware, it more importantly serves as a building block for additional technologies, such as Multiple Input Multiple Output communications techniques and Cognitive Radio, which address the MANET issues of connectivity, bandwidth, and survivability.

Multiple Input Multiple Output (MIMO), as its name suggests, utilizes multiple input and output channels with multiple antenna and receiving/transmitting units to send data in parallel to increase bandwidth by as much as 10 to 20 times the capacity of a traditional single input single output (SISO) radio.[44] MIMO techniques utilize spatial multiplexing, or multi-path, to distribute a single high rate signal among multiple lower rate signals from an array of antennas. Sufficient spacing of the antennas at the transmission and receiving nodes allows the lower rate signals to be differentiated as parallel signals that can be reassembled at the receiver. This provides a large number of virtually parallel channels with a higher signal to noise ratio. Additionally, MIMO technologies can be used to trade off capacity for low power operations that greatly enhance AJ and LPI characteristics of a radio, or to allow a larger number of simultaneous channels to be used.[45] MIMO techniques are the basis of the upcoming 802.11n standard and are the primary enablers of the new standard's planned 100+ Mbps of bandwidth.[46] Under the Mobile Networked MIMO program, DARPA sponsored researchers are exploring methods for incorporating MIMO radio techniques into MANET architectures and have already completed a small-scale Mobile MIMO experiment at speeds of up to 40 mph.[47] The challenge of MIMO in the MANET realm lies in the effects of motion on both a transmitting and receiving array and the need for a minimal amount of antenna spacing at the transmitting and receiving nodes. Mobile MIMO may sacrifice some bandwidth as compared to a static implementation, but the underlying principles remain relevant for MANETs. From an antenna array spacing perspective, the on-going trends in electronic miniaturization have limits in their applicability to MIMO applications. MIMO techniques require a minimum antenna separation on the order of 0.4 of the wavelength of the carrier signal.[48] Therefore, MIMO applications will dictate a minimum size for the physical nodes that utilize the technique. For most vehicle mounted MANET applications, the minimum antenna spacing will not be a significant factor. However, micro or nano scale unattended sensors or UAVs may be limited in their ability to implement MIMO techniques. Additional research into smart antenna and adaptive filtering techniques will be critical to the successful integration of this technology into NCW MANETs (see Appendix C). The disadvantage of MIMO is the additional complexity it brings to the R/T portion of a radio. Fortunately, the MEMS and NEMS based trends in ADCs and DACs that are critical to SDRs will help mitigate this problem. Additionally, as SDRs approach single chip implementations in 10-15 years, multiple SDR "slices", each with a single R/T, could be integrated into an array to create a system level MIMO implementation. This approach would also potentially improve the system performance by distributing the processing load for integrating MIMO data streams amongst multiple SDR slices. No matter the final method of integration, MIMO will allow significant improvements to the connectivity and bandwidth characteristics of MANETs in the future.

The merging of radio and computing that yields SDRs also opens the door to vastly more efficient usage of radio spectrum that can potentially break through the current regulatory bottleneck of spectrum allocation. In the US, the FCC allocates segments of the RF spectrum for use by specific communications devices: AM and FM radios, short wave radios, citizens bands (CB) radios, VHF and UHF television channels, GPS trackers, cellular and cordless phones, et cetera.[49] The strict segmenting of these frequencies was originally driven by a need to reduce interference between users and by the inherent limitations of the early analog electronic technologies in frequency stability and tunability. Today, although several of these bands, most notably the cellular bands, are highly crowded, many more are sparsely used, or may be completely empty in certain areas of the country. According to the FCC's chief engineer, at any given time only about 5 to 10 percent of the entire RF frequency up to 100 GHz is being used, "so there's 90 GHz of available bandwidth."[50] By utilizing the vastly increasing computing capabilities of SDR architectures, a future radio will be able to tap into this bandwidth through its ability to "sense its environment and location and then alter its power, frequency, modulation and other parameters so as to dynamically reuse available spectrum."[51] This extension of SDR is known as cognitive radio.

Cognitive Radio (CR) technologies hold great promise for addressing the pressing bandwidth needs of both the commercial and defense sectors. The basic premise of a CR is based on two core capabilities: 1) the ability to sense the RF environment to find unused spectrum to transmit in and 2) the complementary ability to detect when another user begins to transmit at that frequency and then quickly jump out to a different frequency. The second capability, user detection and frequency agility, is a direct outgrowth of core SDR capabilities and require no additional substantial technologies. Implementing the sensing capability of CR, however, requires the radio to monitor RF usage and activity across broad bands of the spectrum over time and, in the case of a MANET implementation, over varying geographies. In short, CRs must possess situational awareness including self-knowledge of location. CRs will leverage MIMO techniques, for not only the improved bandwidth and connectivity, but because the multi-path signal properties that MIMO is based on also yield important spectral-spatial information to the CR.[52] Though this need for situational awareness drives additional processing requirements, it also provides an ancillary benefit to the military domain. Since they will be constantly collecting and evaluating the RF spectrum around them, each CR in a MANET will effectively act as a sensor that can contribute to its node's, and therefore the overall combat enterprise's, situational awareness and directly contribute to mission completion.[53] Related to the core CR principles, DARPA is also pursuing "policy-based" control protocols for CRs that will allow for better knowledge of and de-confliction of spectrum allocation outside of the US. Under the Next Generation (XG) Communications Program, DARPA plans to provide a cognitive structure that acts as an agent for storing, managing, and de-conflicting local spectrum allocation policies for CRs. By taking advantage of a CR's knowledge of its geographic location, XG agents in the radio will optimize spectrum usage by keeping the radio out of restricted frequencies for that region, or by tracking and negotiating spectrum use of licensed frequencies to enable leasing or micro-charging arrangements.[54] The XG approach is also applicable to a larger CR problem of minimizing interference to "legal" users of spectrum. In the basic CR approach, a radio, after finding an apparently available piece of spectrum, begins broadcasting and, unbeknownst to it, interferes with another radio that has been monitoring that frequency for a licensed broadcast. This scenario is of significant concern to spectrum regulatory agencies such as the FCC. By tracking spectrum use policy based on geography, the XG program hopes to minimize the occurrences and consequences of inadvertent interference as described above. From a military perspective, XG based CRs would also be a significant boon in facilitating interoperability with coalition partners' communications systems.[55]

From a radio perspective, future MANETs will enjoy the fruits of an alignment of needs between the commercial sector, the DoD, and the FCC, to greatly expand the connectivity and bandwidth of wirelessly networked devices. The joint interest in the technologies of SDR, MIMO, and CR, should easily provide the radio centric capabilities that are necessary for MANET implementation of NCW principles. However, the other component of MANET capabilities, the network, faces several challenges that must be overcome if we are to achieve the vision of NCW by 2025.

Network related challenges and research efforts

In contrast to the radio technologies, where a clear synergy exists between the commercial and defense markets, the growth in networking related technologies has been dominated by commercial applications, predominately centered on connectivity to, and compatibility with, the Internet. As TCP/IP is the *lingua franca* of the Internet, it has become the protocol of choice amongst commercial networking equipment vendors. Unfortunately, from a MANET perspective, TCP/IP was designed around a stable, strongly connected, predictable network and its routing protocol is based on these assumptions. The reality of MANETs is quite different, making TCP/IP a poor choice for MANET implementation. In addition to the issues derived from use of these protocols, the ability of MANETs to perform adequately, or even exist at all, on the scale demanded by NCW proponents is simply unknown. Finally, the numerous security concerns – viruses/worms, unauthorized access, data integrity, etc. – that plague the Internet, are just as much threats to MANETs. Although space does not permit inclusion of the security implications in this paper, the reader is referred to Appendix C for this discussion. We now begin our overview of trends and challenges in networking technologies and discuss their effectiveness in meeting our objective MANET characteristics of connectivity and bandwidth.

Despite the anticipated improvements in connectivity derived from software defined radios utilizing cognitive radio and MIMO capabilities as described in the previous section, MANETs, by their very nature, will suffer node disconnects. Knowing this, it is critical that the underlying networking protocols are able to adapt and maintain network coherence without incurring significant impacts to the network's performance. Currently, the widely used TCP/IP protocol presents a challenge for MANETs as it requires knowledge of the destination address before a message is sent and then the continued presence of the destination node at that address until it is delivered. Due to the dynamics of MANET environments, both of these requirements are issues. First off, maintaining current routing tables requires a large amount of overhead communications as the nodes move in and out of the net or from one sub-net to another. Second, once a message is transmitted, the message is dumped if the destination node leaves the network even if the destination node quickly rejoins. Both of these issues are being addressed under the auspices of Delay-/Disruption-Tolerant Networking (DTN) initiatives. DTN researchers have identified four technology needs to supplement current routing protocols to address these issues: bundling, fuzzy scheduling, late binding, and reasoning-based resource planning and utilization.[56] Bundling is a store-and-forward concept in which a message may be held at a routing node for a period of time while waiting for the next node in the route to become available. Fuzzy scheduling uses AI techniques to make routing decisions with limited path information. Late binding refers to the binding of the destination address to the message. In TCP/IP, address binding occurs before message transmission, as discussed above. Late binding would allow the message to begin its journey without knowledge of its destination address and permits discovery of the destination IP address as it is routed through the network.[57] Fuzzy scheduling and late binding are focused more on assured delivery than on finding optimum routes; they trade latency for connectivity. Reasoning-based resource planning and utilization technologies allow a MANET to make routing decision while taking into consideration specific node advantages or disadvantages using a rules set. For example, a node on a powered vehicle would be preferred to a node that is an unattended sensor with a life-limiting battery power source. DTN in general, and bundling and late binding in particular, are relatively straightforward and widely embraced concepts in the internetworking community to the point of being the subject of a recent Internet Engineering Task Force Network Working Group Request for Comments memo.[58] These capabilities should easily be available in the 2025 timeframe. The fuzzy scheduling and reasoning-based resource planning concepts are also widely discussed, but there is currently little consensus on a path-forward. However, it seems reasonable to assume, based on the implicit processing capability and inherent situational awareness of CRs, that one or more of the large number of candidate MANET routing protocols based on fuzzy logic principles[59] will prove capable of addressing this connectivity problem by 2025. The uncertainty in this assumption, however, lies in what the appropriate OSI layer is for integrating these solutions, and to what degree they become a part of networking standards. An ideal outcome would be incorporation of these capabilities into the core IP standard. While this cannot be considered a given, the growing potential user base for MANET technologies and ubiquitous computing and sensor nets will lend some weight to this possibility. Another critical networking capability that CRs enable relates to the four network performance characteristics that we discussed in the Network Theory section. Through their knowledge of the nearby network composition, networking algorithms could be designed that allow neighboring CRs to collectively select local link topologies that provide favorable clustering, link/node ratios, and skew distribution of links. Consciously adapting the local topology, rather than simply linking to every node in range, could greatly enhance overall MANET performance. This ability to specify the topology of a MANET could also prove to be crucial if limitations in the scalability and total capacity of MANETs are found to exist.

As interest (not to mention funding) associated with the NCW fueled vision of a vast network of networks consisting of literally thousands of nodes grew in the late 1990s, networking researchers began to take a hard look at the physics and mathematics of MANET capacity. In early 2000, two engineers from the University of Illinois at Urbana-Champaign published a paper that claimed the capacity of a static 802.11 based ad hoc wireless network scales as *n*/sqrt(*n*), meaning that as a network increased in number of nodes, *n*, the capacity in terms of bandwidth approached zero.[60] A flurry of additional research followed showing that network capacities could be improved by selecting different approaches to the problem, or by using novel techniques with questionable applicability to MANET implementations.[61] These findings were positive, but each addressed only a portion of the MANET problem space and it remained unclear as to what the overall MANET capacity boundary might be. So in early 2006, DARPA stood up a new program called Information Theory for MANETs (ITMANET), with the intent of solving the "Grand Challenge in MANET Information Theory: Precise characterization of MANET capacity with a unified accounting for mobility, uni/multi/omnicast, latency, topology, energy, and multiuser issues."[62] By considering all of the physical and algorithmic dimensions of MANET variability, this effort seeks to establish a firmer theoretical foundation to enable meaningful modeling and simulation of various MANET configurations. This is a critical need for addressing some basic questions about the achievability of the core NCW tenet of a fully networked force. As more and more of our diminishing DoD budget gets allocated to

NCW premised systems it is vital that we gain a better understanding of the underlying limits of this family of technologies so that we may answer the most basic NCW question; is a large scale, robust MANET achievable? The ITMANET program is scheduled to complete in 2011[63], but this timeline must be taken with a grain of salt. However, even if the ITMANET program is unable to achieve its ultimate goal, the increased understanding of the various MANET dimensions will provide valuable insights into the scalability and bandwidth capacities of MANETs. For, as we noted in our objective MANET discussion, connectivity without bandwidth is of little combat value.

Summary and Recommendations

The tenets of NCW are the fabric of the DoD's transformation efforts and the drivers for several of the Department's largest acquisition programs. By adapting a network-centric culture, organizational structure, and doctrine, and by embracing information technology to interconnect all the components of the DoD enterprise, we can use the resultant shared situational awareness to achieve information superiority. This information superiority will enable agile employment of a lighter, leaner, more lethal combat enterprise that overwhelms any potential adversary before they respond. In order to achieve the totality of this vision, we must robustly connect not just the core C4ISR centers, but all of the sensors, soldiers, vehicles, and aircraft – the tactical warfighting nodes – as well. Achieving this tactical edge connectivity will depend on the development of significantly improved MANET technologies.

Beginning with an examination of the fundamentals of networking and network theory, the basics of wired and wireless computer networks were examined as a lead-in to the specific advantages and disadvantages of MANETs. After defining the characteristics of an objective MANET in terms of connectivity, bandwidth, survivability, and security, an analysis of the challenges and projected trends in MANET related technologies was undertaken.

Viewed from the vantage point of the year 2025, our review of challenges and trends in research on radios and networking identified several key enabling technologies that will be critical to achieving the characteristics of our objective MANET. Specifically on the radio side, the foundational technology of software defined radios (SDR) was judged as being strongly supported by both the commercial and defense markets. Achieving the necessary SDR capabilities envisioned for our 2025 timeframe is considered to be a low risk and does not require any additional funding beyond the levels already planned to support near term JTRS related acquisitions. Building upon SDRs, the technologies of multiple input multiple output (MIMO) receiver/transmitters and cognitive radio (CR) also enjoy broad base support in the commercial sector. However, moving CR forward in a timely manner would be greatly aided by continuing DoD pressure on the FCC (which is already inclined to support CR) to create a streamlined CR certification process, and by increased targeted investments in CR algorithm development and testing efforts at government labs and universities.

The true challenges and the potential for the biggest risks to achieving the required MANET capabilities lie in the networking technologies. The current fundamental Internet routing protocol, TCP/IP, is completely inadequate to meet the needs of MANETs. Driven primarily by DoD requirements, the academic community is engaged in pursuing MANET purposed routing technologies. This fact, combined with the inherent geographic and RF-environment situational awareness that future CRs will enable, tends to reduce, but not mitigate, this risk. Although it is reasonably certain that adequate routing solutions will be found by 2025, it is decidedly less certain as to how easily that solution will integrate into COTS networking solutions. Given the DoD’s poor previous cost track record with proprietary communications solutions, this risk seems to warrant a low level, long range investment in this area. Finally, the largest risk to large scale MANET implementation is the uncertainty in the ultimate scalability and capacity of MANETs due to a fundamental lack of a consolidated theory for MANET behavior. Without continued advancement along the path of information theory related to this networking application, the acquisition community will not be able to utilize meaningful modeling and simulation techniques to assist in designing and selecting the protocols and architectures that will underlie the envisioned large scale MANET necessary to bring the NCW to reality. The Air Force should immediately fund basic research in this area at government labs and universities.

Appendix A: Five Characteristics of Network Performance

In the Networks and Network Theory section of this paper, we introduced five measures that can be used to characterize network performance. These measures are borrowed from the Complex Network Primer appendix[64] of Jeff Cares' excellent book, *Distributed Networked Operations: The Foundations of Network Centric Warfare*, to which the reader is referred for further discussion.

1. Characteristic Path Length (CPL) – The median of the average distance from each node to every other node in a network.[65] To calculate CPL, measure the number of links from node 1 to node 2, then node 1 to node 3, and on, up to node 1 to node N. Average all these values for node 1. Now go to node 2 and repeat the process. At the end, you will have N number of average distances. Arrange these values in order from shortest to longest and find the median value. This value is the CPL for that network. Shorter CPLs equate to lower latency, as fewer hops are required to pass data from a given node to another.

2. Link/node ratio – Simple ratio of total number of links to total number of nodes in a given network.

3. Clustering – A measure of local cohesion in a network. This measure is expressed as a clustering coefficient, γ. The clustering coefficient is determined by selecting a node, k, determining which nodes are neighbors of k, and then the ratio of the number of actual links between k's neighbors to the possible number of links between k's neighbors. If all of k's neighbors are also connected to one another, then $\gamma(k) = 1$. If none of k's neighbors are connected to each other, then $\gamma(k) = 0$. The clustering coefficient for a network is the average of the clustering coefficients for each node in the network. Adaptive networks have a skew distribution of their local node cluster coefficients.[66]

4. Scale – A measure of how links are distributed among nodes in a given network.[67] If every node in a network has an approximately equal (i.e. uniform) number of links, then the network is said to exhibit scale. In scale free networks, the links have a skew degree distribution among the nodes. Networks with scale tend to be less robust to the loss of a few random nodes than scale free networks, as the loss of a random node from a scale network will always remove a fixed percentage of links. Random node removal from a scale free, or skew network, is likely to remove only a small number of links, as most nodes have very few links. It should be noted that the targeted removal of high degree nodes (i.e. nodes with a large number of links) is much more devastating to a scale free network than a scale network.

5. Diffusion rate – The average number of nodes in a network that are reachable by traveling exactly *l* links.[68] Diffusion rates are typically expressed as graphs of the number of nodes reached versus number of links traveled. The steeper the curve of the graph, the higher the diffusion rate of the network.

Appendix B: Application of MANET Technologies for NCW in Blue Horizons scenarios

As part of the larger Blue Horizons research effort, two ACSC students, Maj Joel "Spicoli" Luker and Maj James "Buster" Myers, jointly developed two, two-axis models of potential threats for use as contextual tools to evaluate the respective technology areas that the remaining Blue Horizons students were investigating. Maj Luker fleshed out scenarios assuming state actors against a matrix of material dominant vs. information dominant and foreign soil vs. US soil. Maj Myers developed scenarios assuming non-state actors in a matrix of material dominant vs. information dominant and regular vs. irregular warfare.

Using the scenario specifics for each quadrant in their matrices, I will briefly discuss relevant features of MANET technologies in the context of NCW forces, as either positive or negative contributors to each quadrant. Readers are referred to Maj Luker's[69] and Maj Myers'[70] respective papers for the full background on each scenario. I will begin with Maj Luker's state actor scenarios.

Wishful Thinking: Regular Warfare Against a Materials-Based Adversary

NCW forces would fare well in this scenario, despite the anticipated loss of a significant portion of US space capabilities. The communications satellites that provide link back into the GIG for MANET connected forces will remain relatively unscathed in their geosynchronous orbits. The loss of imagery satellites and projected improvements in anti-air capabilities would put a premium on the MANET enabled intelligence gathering capabilities of NCW forces and expendable unattended sensors.

Information Immobilization: Regular Warfare Against an Information-Based Adversary

This is essentially a NCW on NCW enabled force scenario, with the US still retaining an advantage in firepower. This type of scenario would be very taxing for MANET connected forces, as the adversary would be well aware of the vulnerabilities and capabilities of our networks. This situation is cautionary for NCW zealots, since as we put greater and greater reliance on our networks as the primary enabler of our military capabilities, our individual platforms and weapon systems could become practically useless if the networks are neutralized.

David and Goliath: Irregular Warfare Against a Materials-Based Adversary

MANET technologies combined with widespread use of unattended sensors could be an important aspect of the US reaction to this scenario, though the adversaries focus on non-military IOPS clearly marginalizes much of NCW's utility.

The Phantom Menace: Irregular Warfare Against an Information-Based Adversary

NCW would not be particularly relevant in this scenario as the adversary's target set is focused on economic and political effects.

We now turn to Maj Myers' Non-state actors scenarios.

American Insurgency: Material Dominant on Our Soil

MANET enabled forces will contribute significantly to the ISR fight, which will be critical in identifying insurgent leadership and detect preparation and execution of terrorist acts. Again, not a war winner, but a significant improvement on current capabilities in this area.

Cyber 9/11: Information Dominant on Our Soil

NCW infrastructure, including MANETs, would be a prime target in this scenario, underscoring the warning that was offered in the Information Immobilization scenario above.

Blind Battlefield: Information Dominant on Foreign Soil

Common to the other information dominant scenarios, the NCW infrastructure would be targeted in an attempt to attrit our combat capablities. However, this scenario assumes that several core NCW tenets, such as transition to network organizations, do not occur, and therefore theoretically eliminates some core NCW capabilities and features such as self-synchronization and cooperative engagement. Accepting the assumption as valid, MANET technologies would serve primarily as means to feed information back to centralized C2 nodes which are specifically targeted by the adversary. Hypothetically, MANETs could enable US forces to reform and rally despite the loss of their centralized control mechanisms. This is difficult to evaluate given the antithetical NCW assumptions that were presented.

Guerillas in the Mist: Material Dominant on Foreign Soil

By greatly reducing or even eliminating prominent C4ISR targets from the battlespace, NCW forces enabled by MANETs could largely negate this adversary. In addition to removing an important friendly vulnerability, NCW forces would again, similar to the American Insurgency scenario, be able to provide greatly improved ISR to dissuade and discourage the Insurgent efforts.

Appendix C: Areas for Further Investigation

The range of information technologies that converge in the MANET application area and the limited scope of this paper did not permit a thorough examination of many relevant technology areas. Below is a short listing (by no means exhaustive) of potential technology areas that need additional attention and development in order to achieve the vision of NCW MANETs.

Application tuning: Ultimately, the bandwidth requirements for a MANET or any network are driven by the applications that ride on them. The NCW vision of vast networks of sensors, shooters, decision makers, and influencers[71] provides for the possibility of an almost limitless amount of source data. Getting this data to the right user/application has been addressed by Alberts and Hayes in *Power to the Edge*. They propose architectures that support post before processing policies which post raw data as soon as its available and without waiting for any processing to occur.[72] All other nodes that may be interested in that data will then pull it from the source node. From a MANET perspective, this policy proposal must be balanced against the potential bandwidth impacts. If a mobile node acquires a particularly "interesting" set of data, it would be useful to quickly push it to a more advantaged node (in terms of bandwidth) so as not to flood the typically more constrained MANET with numerous requests for that data set. This is an example of application tuning. Other examples include traditional techniques such as data compression. Application tuning will likely result in higher costs in terms of processing requirements and acquisition timelines, so a cost benefit analysis will likely be required for each significant bandwidth intensive application. Note that these cost-benefit analyses will be greatly facilitated by successful completion of the DARPA ITMANET program discussed above.

Artificial Intelligence: AI advances in areas such as link selection, optimal routing, and network self-monitoring hold great promise. The debate of whether such AI should be embedded in the network itself, rather than in individual nodes, will be driven on improvements in processing power vs. algorithmic efficiency and on assumptions on MANET scalability and density in a given operational are. In the end, a hybrid approach of certain AI technologies residing in the network layer and other residing in the application layer on individual nodes would seem to be the likely outcome.

Battery technologies: Unattended sensors and man portable configurations will require improved battery technologies to provide optimum utility. DARPA's Connectionless Networking program is addressing this issue from the sensor perspective, but it is not applicable to dismounted operations for MANETs.

Multi-Level Security (MLS) Policy Management: Implementing networks that autonomously manage MLS policy management is a Holy Grail for C2. Trusted computing and neural net based AI hold some promise in this area, but it will likely remain a source of inefficiency and a significant chokepoint for truly embracing NCW for the foreseeable future. As this is a motherhood military networking issue that is not specific to MANETs, I gladly leave this issue to be addressed by wiser, more patient students than I.

Network Security: Security issues for wireless networks could easily fill an entire paper on their own. Every security issue that cabled networks have (viruses, worms, denial of service attacks, etc.), wireless networks and MANETs have as well. Although the upcoming IPv6 addresses several security holes in IPv4 (the current Internet IP implementation), it unfortunately introduces several new ones. Since the exposed nature of wireless links leave them open to exploitation by virtually anyone with limited exposure to themselves, add-on encryption in the form of VPNs or external bulk signal encryption will likely remain a fact of life for MANETs for the foreseeable future. These security measures come with a cost of additional processing load (for VPNs) and additional bandwidth requirements (for both). External encryption also add significant bulk and power requirements especially for unattended sensors and micro/nano UAV implementations. Because of this, there will be a continual need to balance operational security requirements against loss of potentially valuable data sources.

Open air laser links: Laser communications have many advantages over RF – higher potential bandwidth (with multiplexing), excellent LPI/LPD properties, longer range – but also suffer from many disadvantages. The need for direct LOS, relatively clear air, precise knowledge of the location of the intended recipient (especially difficult when both nodes are moving), and the relative fragility of laser optics in general make for a challenging set of limitations to overcome for widespread application in MANETs.

Smart antenna design: Several MEMS and NEMS techniques are under consideration for tunable antennas designs. These technologies can potentially make drastic improvements on bandwidth, and connectivity, as well as enhancing LPI/LPD capabilities.

Bibliography

"How Bluetooth Technology Works." *Whitepaper at http://www.bluetooth.com/Bluetooth/Learn/Works/*

"Information Processing Systems – OSI Reference Model – The Basic Model." ISO Standard ISO/IEC 7498-1:1994(E) *at http://www.sigcomm.org/standards/iso_stds/OSI_MODEL/ISO_IEC_7498-1.TXT*, 1994.

"What is Software Defined Radio?" *SDRForum.org at http://www.sdrforum.org/pages/aboutTheForum/faqs.asp*

Adams, James. *The Next World War*. New York, NY: Simon & Schuster, 1998.

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare*. Washington DC: Command and Control Research Program, 2003.

Alberts, David S., and Richard E. Hayes. *Power to the Edge, Information Age Transformation*. Washington DC: Command and Control Research Program, 2004.

Anderson, Sharon and Stephen Davis. "The Joint Tactical Radio System – Reloaded." *CHIPS*, July-September 2006: 6-9.

Arquilla, John, and David Ronfeldt. *In Athena's Camp*. Santa Monica, CA: RAND, 1997.

Ashley, Steven. "Cognitive Radio." *Scientific American.com at http://sciam.com/article.cfm?chanID=sa006&articleID=000C7B72-2374-13F6-A37483414B7F0000&pageNumber=1&catID=2*, February 20, 2006.

Asokan, A., Kari Kostiainen, Philip Ginzboorg, Jorg Ott, and Cheung Luo. "Towards Securing Disruption-Tolerant Networking." Whitepaper *at http://research.nokia.com/tr/NRC-TR-2007-007.pdf*, March 21, 2007.

Ballah, Jason T. "Integrated Manet Mutual Authentication System." Wright-Patterson AFB, OH: Air Force Institute of Technology, 2002.

Baras, John S. and Tao Jiang. "Dynamic and Distributed Trust for Mobile Ad-Hoc Networks." Paper presented at 24th Army Science Conference, Orlando, FL, 2004.

Berger, Alex. "The Low-Tech Side of Information Warfare." *Air & Space Power Journal – Chronicles Online Journal at http://www.airpower.maxwell.af.mil/airchronicles/cc/berger.html*, 1998.

Bey, Christopher S. "Airborne Tactical Data Network Gateways: Evaluating EPLRS' Ability to Integrate with Wireless Meshed Networks." Monterey, CA: Naval Post Graduate School, 2005.

Brachman, Ron. "The Heart of the Mind." Paper presented at the DARPATech 2005, 2005.

Brenner, Pablo. "A Technical Tutorial on the IEEE 802.11 Protocol." *Whitepaper at http://www.sss-mag.com/pdf/802_11tut.pdf*, July 18, 1996.

Burgess, John, Brian Gallagher, David Jensen, and Brian Neil Levine. "MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks." Paper presented at IEEE INFOCOM 2006, 2006.

Burr, A. G., M. H. Capstick, B. Kemp, and B. Wang. "Multiband MIMO Antenna Arrays." *IEE Seminar Digests* (2005) at *http://www.iee.org/OnComms/pn/antennas/Bin%20Wang.pdf,* pages 135-139

Cares, Jeff. *Distributed Networked Operations: The Foundations of Network Centric Warfare*. Newport, RI: Alidade Press, 2005.

Cebrowski, Arthur K., and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." *Naval Institute Proceedings* (1998): 28-35.

Cheung, Humphrey. “FBI Teaches Lesson In How To Break Into Wi-Fi Networks.” *InformationWeek.com at http://www.informationweek.com/management/compliance/160502612*, April 7, 2005.

CJCS. “Joint Vision 2010.” Joint Staff.

_____. “Joint Vision 2020.” Joint Staff.

Cox, John. “Communicating Even When the Network’s Down.” *NetworkWorld.com at http://www.networkworld.com/news/2006/111606-dtn.html?page=1*, November 16, 2006.

Deffree, Suzanne. “802.11n: The Next WLAN Frontier.” *EDN.com at http://www.edn.com/article/CA445702.html*, August, 19, 2004.

Ellis, Christopher. “Leveraging IPv6 Capabilities to Facilitate the Deployment of Mobile Ad Hoc and Sensor Networking.” Paper presented at IPv6 Summit 2004, 2004.

Farrell, Stephen, Vinny Cahill, Dermot Geraghty, Ivor Humphreys, and Paul McDonald. “When TCP Breaks: Delay- and Disruption-Tolerant Networking.” *IEEE Internet Computing at http://dsonline.computer.org/portal/site/dsonline/menuitem.9ed3d9924aeb0dcd82ccc6716bbe36ec/index.jsp?&pName=dso_level1&path=dsonline/2006/08&file=w4spot.xml&xsl=article.xsl&*, July/August 2006

FCC. “Authorization and Use of Software Defined Radios.” ET Docket No. 00-47 *at http://www.fcc.gov/Bureaus/Engineering_Technology/Orders/2001/fcc01264.txt*, Washington DC, September 14, 2001.

Fette, Bruce. “Cognitive Radio Shows Great Promise.” *COTS Journal at http://www.cotsjournalonline.com/home/article.php?id=100206&pg=1*, October, 2004.

Fordigh, Magnus & Per Johansson & Peter Larsson. "Wireless Ad Hoc Networking - the Art of Networking without a Network." *Ericsson Review 4* (2000): 248-63.

Ghosh, Anup. "Defending Warfighter Networks." Paper presented at the DARPATech 2005, 2005.

Government Accountability Office. "The Global Information Grid and Challenges Facing Its Implementation." GAO, 2004.

Griggs, Stephen. “Mobile Networked MIMO (MNM) Program.” Paper presented at DARPA’s WANN Proposer’s Day, 2006.

Gunning, David. "Learning and Reasoning: The True Heart of the Mind." Paper presented at the DARPATech 2005.

Gupta, P. and P. R. Kumar. “The Capacity of Wireless Networks.” *IEEE Transactions on Information Theory* (March, 2000): 388–404.

Holland, Charles. "Broadening the Scope." Paper presented at the DARPATech 2005, 2005.

Joe, Leland and Isaac Porche III. *Future Army Bandwidth Needs and Capabilities*. Santa Monica, CA, RAND, 2004.

Johnson, Stuart E., and Martin C. Libicki. *Dominant Battlespace Knowledge*. Washington DC: National Defense University, 1996.

Kenyon, Henry S. “Smart Radios Juggle Spectrum.” SIGNAL *at http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=48&zoneid=22*, December 2003.

Khalilzad, Zalmay M., and John P. White. *The Changing Role of Information in Warfare*. Santa Monica, CA: RAND, 1999.

Kurzweil, Ray. *The Singularity is Near: When Humans Transcend Biology*. New York, NY: Penguin Books, 2005.

Latt, Khine. "Naval Supremacy." Paper presented at the DARPATech, 2005.

Luker, Joel. J. “State Actor Threats in 2025.” Maxwell AFB, AL: Air Command and Staff College, 2007.

Maeda, Mari. "Making the Most of Sensing and Experiencing for the Next Patrol." Paper presented at the DARPATech 2005.

Mannion, Patrick. “Sharing Spectrum the Smarter Way.” *EETimes.com at http://www.eetimes.com/article/showArticle.jhtml?articleId=18700443*, April 5, 2004.

Marsh, David. "Software Defined Radio Tunes In." EDN (2005): 52-63.

Marshall, Preston. “Connectionless Networks Program Overview.” Paper presented at DARPA’s WANN Proposer’s Day, 2006.

Marshall, Preston, “Disruption Tolerant Networking (DTN) Program Overview Brief.” Paper presented at DARPA’s WANN Proposer’s Day, 2006.

Marshall, Preston. "Robust Tactical Networks." Paper presented at the DARPATech 2005, 2005.

Marshall, Preston. "Wireless Adaptable Network Node (WANN)." Paper presented at DARPA’s WANN Proposer’s
Day, 2006.

Marshall, Preston. “XG Communications Program Information Briefing.” Paper presented at DARPA’s WANN Proposer’s Day, 2006.

Milicic, Gregory J. "An Analysis of Hardware Requirements for Airborne Tactical Mesh Networking Nodes." Monterey, CA: Naval Postgraduate School, 2005.

Myers, James W. “Non-State Actor Threats in 2025: Blue Horizons Scenarios.” Maxwell AFB, AL: Air Command and Staff College, 2007.

Myers, Margaret E. "Power to the Edge: Transformation of the Global Information Grid." *CHIPS*, Summer 2002.

Newman, M. E. J. “The Structure and Function of Complex Networks.” *SIAM Review 45*, 2003: 167-256.

Network Working Group. “Delay-Tolerant Networking Architecture.” RFC:4838 *at http://www.rfc-editor.org/rfc/rfc4838.txt*, April 2007.

North, Rich, Norm Browne, and Len Schiavone. “Joint Tactical Radio System – Connecting the GIG to the Tactical Edge.” Paper presented at Military Communications Conference, Washington DC, October 23-25, 2006.

Olive, Joseph. "My Mind to Your Mind." Paper presented at the DARPATech 2005, 2005.

Patterson, Maj Ryan, USMC. "Capturing Live Combat in Network Centric Warfare." Paper presented at the DARPATech 2005.

Princeton, CalTech, Stanford, USC, and Texas. "Mobile Ad-Hoc Networks: Information Theory as a Design Driver." Paper presented at the ITMANET, 7 March 2006.

Ramming, J. Christopher. "Information Theory for Mobile Ad-Hoc Networks (ITMANET)." Paper presented at the ITMANET, 7 March 2006.

Ratnam, Gopal. “Bandwidth Battle.” DefenseNews.com *at http://defensenews.com/story.php?F=2153522&C=airwar*, October 9, 2006.

Saleh, Adel. "Next-Generation Global DoD Enterprise Network." Paper presented at the DARPATech 2005.

Schiavone, Len. “JTRS Overview for CCEB Spectrum Task Force.” *Briefing at http://enterprise.spawar.navy.mil/getfile.cfm?contentId=1488&type=R*

Schwartau, Winn. *Information Warfare*. New York, NY: Thunder's Mouth Press, 1996.

Silbaugh, Eric E. “Network-Centric Operations – Promise, Chimera, and Achilles’ Heel: Challenges and Pitfalls for Networks and Information Infrastructure.” Maxwell AFB, AL: Air Command and Staff College, 2005.

Stubblefield, Adam, John Ioannidis, and Aviel D. Rubin. “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP.” AT&T Labs Technical Report TD-4ZCPZZ, August 6, 2001.

Surman, Glenn. “Understanding Security Using the OSI Model.” Whitepaper at *http://www.sans.org/reading_room/whitepapers/protocols/377.php*, March 20, 2002.

Swami, Ananthram. "Army Perspective on M3awnets." Paper presented at the ITMANET, 7 March 2006.

Toffler, Alvin & Heidi. *War and Anti-War*. New York, NY: Warner Books, 1993.

US Army. “Future Combat System (Brigade Combat Team (FCS(BCT)) 14+1+1 Systems Overview.” *Whitepaper at http://www.army.mil/fcs/whitepaper/FCSwhitepaper07.pdf*, US Army: March 14, 2007.

US Navy. “FORCEnet: A Functional Concept for the 21st Century.” Washington DC: US Navy, February, 2005.

Wagner, Tom. "We Are Not Alone." Paper presented at the DARPATech 2005.

Waltz, Edward. *Information Warfare Principles and Operations*. Boston, MA: Artech house, 1998.

Watkins, Damian. "Tactical Manet Attack Detection Based on Fuzzy Sets Using Agent Communication." In 24th Army Science Conference, Orlando, FL, 2005.

Weiner, Tim. “Pentagon Envisioning a Costly Internet for War.” *NYTimes.com at http://www.nytimes.com/2004/11/13/technology/13warnet.html?ex=11176733976&ei=1&en=04b67210110290e6*, November 13, 2004.

Yoon, Barbara. "Getting to the Heart of the Mind." Paper presented at the DARPATech 2005.

Notes

[1] CJCS, “Joint Vision 2010.” (Joint Staff) and CJCS, “Joint Vision 2020.” (Joint Staff).

[2] Arquilla, John, and David Ronfeldt. *In Athena's Camp*. (Santa Monica, CA: RAND, 1997) page 24

[3] Berger, Alex. “The Low-Tech Side of Information Warfare.” *Chronicles Online Journal*

[4] Silbaugh, Eric E. “Network-Centric Operations – Promise, Chimera, and Achilles’ Heel: Challenges and Pitfalls for Networks and Information Infrastructure.” (Maxwell AFB, AL: Air Command and Staff College, 2005)

[5] US Army. “Future Combat System (Brigade Combat Team (FCS(BCT)) 14+1+1 Systems Overview.” (March 14, 2007) page 2

[6] US Navy. “FORCEnet: A Functional Concept for the 21st Century.” (February, 2005) page 5

[7] Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare*. (Washington DC: Command and Control Research Program, 2003) page 187

[8] Cebrowski, Arthur K., and John J. Garstka. “Network-Centric Warfare: Its Origin and Future.” *Naval Institute Proceedings* (1998)

[9] Ibid, page 28

[10] Alberts, David S., and Richard E. Hayes. *Power to the Edge, Information Age Transformation*. (Washington DC: Command and Control Research Program, 2004) page 125

[11] Ibid, page 127

[12] Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare*. (Washington DC: Command and Control Research Program, 2003) page 88

[13] Ibid, pages 157-183

[14] Ghosh, Anup. "Defending Warfighter Networks." (DARPATech 2005) page 25

[15] Newman, M. E. J. “The Structure and Function of Complex Networks.” (*SIAM Review 45*, 2003) page 168

[16] Ibid, page 171

[17] Cares, Jeff. *Distributed Networked Operations: The Foundations of Network Centric Warfare*. (Newport, RI: Alidade Press, 2005) pages 149-150

[18] Ibid, page 163

[19] Ibid, page 159

[20] Ibid, page 163

[21] Ibid, page 163

[22] “Information Processing Systems – OSI Reference Model – The Basic Model.” (ISO, 1994) section 6

[23] Ibid, section 7.7.2

[24] Marshall, Preston. "Robust Tactical Networks." (DARPATech 2005) page 11

[25] Ibid, pages 11-12

[26] Ibid, page 12

[27] In August 2001, AT&T Labs published a paper that detailed the vulnerabilities with the WEP implementation of RC4 and described the tools and simple methods needed to extract the 128-bit encryption key (Stubblefield, Adam, John Ioannidis, and Aviel D. Rubin. “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP.” (AT&T Labs, August 6, 2001)). In March 2005, the FBI publicly demonstrated how to break a 128-bit WEP in less than 3 minutes with basic

hardware and software available from the Internet (Cheung, Humphrey. “FBI Teaches Lesson In How To Break Into Wi-Fi Networks.” *InformationWeek.com* (April 7, 2005)).

[28] Ratnam, Gopal. “Bandwidth Battle.” DefenseNews.com (2006) page 3

[29] Ibid, page 2

[30] Ibid, page 2

[31] Brenner, Pablo. “A Technical Tutorial on the IEEE 802.11 Protocol.” (July 18, 1996) page 5

[32] “How Bluetooth Technology Works.” *Whitepaper at http://www.bluetooth.com/Bluetooth/Learn/Works/*, page 1

[33] North, Rich, Norm Browne, and Len Schiavone. “Joint Tactical Radio System – Connecting the GIG to the Tactical Edge.” (Washington DC, 2006) page 1

[34] Anderson, Sharon and Stephen Davis. “The Joint Tactical Radio System – Reloaded.” *CHIPS* (July-September 2006) page 7

[35] Ibid, page 7 (sidebar)

[36] “What is Software Defined Radio?” *SDRForum.org at http://www.sdrforum.org/pages/aboutTheForum/faqs.asp*

[37] Marsh, David. “Software Defined Radio Tunes In.” *EDN* (2005) page 53

[38] Ibid, page 53

[39] Ashley, Steven. “Cognitive Radio.” *Scientific American.com* (February 20, 2006) Page 5

[40] Kurzweil, Ray. *The Singularity is Near: When Humans Transcend Biology*. (New York, 2005) pages 61, 63, 64

[41] Marsh, David. “Software Defined Radio Tunes In.” *EDN* (2005) page 62 (sidebar).

[42] FCC. “Authorization and Use of Software Defined Radios.” ET Docket No. 00-47 (Washington DC, September 14, 2001)

[43] Marsh, David. “Software Defined Radio Tunes In.” *EDN* (2005) page 53

[44] Griggs, Stephen. “Mobile Networked MIMO (MNM) Program.” (DARPA 2006) page 3

[45] Ibid, page 6

[46] Deffree, Suzanne. “802.11n: The Next WLAN Frontier.” *EDN.com* (2004) page 1

[47] DARPA’s experiment consisted of one mobile transmitter node with one mobile receiver node using multiple MIMO antenna array configurations. Griggs, Stephen. “Mobile Networked MIMO (MNM) Program.” (DARPA 2006) page 5

[48] Burr, A. G., M. H. Capstick, B. Kemp, and B. Wang. “Multiband MIMO Antenna Arrays.” *IEE Seminar Digests* (2005) page 135

[49] Ashley, Steven. “Cognitive Radio.” *Scientific American.com* (February 20, 2006) page 2

[50] Mannion, Patrick. “Sharing Spectrum the Smarter Way.” *EETimes.com* (April 5, 2004) page 2

[51] Ibid, page 1

[52] Ashley, Steven. “Cognitive Radio.” *Scientific American.com* (February 20, 2006) page 7

[53] Mannion, Patrick. “Sharing Spectrum the Smarter Way.” *EETimes.com* (April 5, 2004) page 2

[54] Marshall, Preston. “XG Communications Program Information Briefing.” (DARPA, 2006) page 3

[55] Kenyon, Henry S. “Smart Radios Juggle Spectrum.” *SIGNAL* (December 2003) page 1

[56] Marshall, Preston, “Disruption Tolerant Networking (DTN) Program Overview Brief.” (DARPA, 2006) page 3

[57] Cox, John. “Communicating Even When the Network’s Down.” *NetworkWorld.com* (Nov 16, 2006) page 3

[58] Network Working Group. “Delay-Tolerant Networking Architecture.” RFC:4838 (April 2007) pages 3-4

[59] BAE presentation at USIPv6 Summit in 2004 defined six categories of MANET routing protocols along with the then current list of specific protocol under each. The breakout was: Proactive Protocols (10), Reactive Protocols (16), Hierarchical Protocols (13), Geographical Protocols (5), Power Aware Protocols (8), Multicast Protocols (20). Ellis, Christopher. “Leveraging IPv6 Capabilities to Facilitate the Deployment of Mobile Ad Hoc and Sensor Networking.” Paper presented at IPv6 Summit 2004, 2004.

[60] Gupta, P. and P. R. Kumar. “The Capacity of Wireless Networks.” *IEEE Transactions on Information Theory* (March, 2000)

[61] Ramming, J. Christopher. "Information Theory for Mobile Ad-Hoc Networks (ITMANET)." (DARPA, 2006) page 11

[62] Ibid, page 11

[63] Ibid, page 15

[64] Cares, Jeff. *Distributed Networked Operations: The Foundations of Network Centric Warfare*. (2005) pages 149-172

[65] Ibid, page 149

[66] Ibid, page 166

[67] Ibid, page 150

[68] Ibid, page 167

[69] Luker, Joel. J. “State Actor Threats in 2025.” Maxwell AFB, AL, Air Command and Staff College, 2007

[70] Myers, James W. “Non-State Actor Threats in 2025: Blue Horizons Scenarios.” Maxwell AFB, AL, Air Command and Staff College, 2007

[71] Cares, Jeff. *Distributed Networked Operations: The Foundations of Network Centric Warfare*. (2005) page 77

[72] Alberts, David S., and Richard E. Hayes. *Power to the Edge, Information Age Transformation*. (2004) page 82